International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3524

(12/2019)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Cloud Computing

Cloud computing maturity requirements and framework

Recommendation ITU-T Y.3524

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	**Y.3500–Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3524

Cloud computing maturity requirements and framework

Summary

Recommendation ITU-T Y.3524 provides the functional framework and requirements for cloud computing maturity. It introduces an overview of cloud computing maturity and identifies the cloud computing maturity model including the cloud customer management module, cloud resource management module, cloud service management module and cloud security management module. Additionally, this Recommendation provides cloud computing maturity requirements derived from use cases.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3524	2019-12-14	13	11.1002/1000/14136

Keywords

Cloud computing, framework, maturity, model, requirements.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3524

Cloud computing maturity requirements and framework

1 Scope

This Recommendation specifies the cloud computing maturity requirements and framework based on relevant use cases. The scope of this Recommendation includes:

1) Overview of cloud computing maturity;

2) Cloud computing maturity framework;

3) Cloud computing maturity requirements;

4) Typical use cases of cloud computing maturity.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601]	Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.
[ITU-T Y.3500]	Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.
[ITU-T Y.3501]	Recommendation ITU-T Y.3501 (2016), *Cloud computing framework and high-level requirements*.
[ITU-T Y.3502]	Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture*.
[ITU-T Y.3517]	Recommendation ITU-T Y.3517 (2018), *Cloud computing – Overview of inter-cloud trust management*.
[ITU-T Y.3521]	Recommendation ITU-T Y.3521/M.3070 (2016), *Overview of end-to-end cloud computing management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.2 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 cloud service user [ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.6 service catalogue [ITU-T Y.3502]: A listing of all the cloud services of a particular cloud service provider.

3.1.7 service level agreement (SLA) [ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.8 resource management [b-ITU-T Y.3520]: The most efficient and effective way to access, control, manage, deploy, schedule and bind resources when they are provided by service providers and requested by customers.

3.1.9 architecture [b-ISO/IEC/IEEE 42010]: Fundamental concepts or properties of a system in its environment embodied in its elements, relationships and in the principles of its design and evolution.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms.

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

anti-DDoS	anti-Distributed Denial of Service
API	Application Programming Interface
BC/DR	Business Continuity and Disaster Recovery
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CCMM	Cloud Customer Management Module
CRMM	Cloud Resource Management Module
CSMM	Cloud Service Management Module
CSEMM	Cloud Security Management Module
DB	Database
ETL	Extract-Transform-Load
FAQ	Frequently Asked Questions
IaaS	Infrastructure as a Service

IAM	Identity and Access Management
IOPS	Input/Output Operations Per Second
SLA	Service Level Agreement
VM	Virtual Machine

5 Conventions

In this Recommendation:

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of cloud computing maturity

Cloud computing maturity is a kind of comprehensive criteria to define the effect and level in adoption of cloud computing. It describes three dimensions: technology, management and effectiveness, and covers partially cloud computing management as defined in [ITU-T Y.3521]: cloud customer management, cloud service management, and cloud resource management. Actually advanced description levels, rather than service level agreements (SLAs) are used to indicate the direction of maturity and to support different roles such as those of cloud service customers (CSCs), cloud service providers (CSPs), etc. to improve cloud computing maturity.

This Recommendation focuses on analysing the cloud maturity framework and functional requirements based on the cloud customer management, cloud service management, resource management and cloud security management.

6.1 Cloud computing maturity model

The aim of cloud computing management is to use the cloud resources efficiently, ensure cloud service stability and CSC:cloud service user flexibility. This Recommendation describes a cloud computing maturity model based on four-module and three-dimensional design that supports management processes independent of the technology used. The matrices of the cloud computing maturity model shown in Figure 6-1 are as follows:

– **Three-dimensions**: The ultimate effectiveness of cloud computing is reflected under the combined effects of technology and management. The three dimensions of cloud computing considered are technology, management and effectiveness. The requirements of maturity are derived from these three dimensions.

– **Four modules**: The model covers a cloud customer management module (CCMM), a cloud service management module (CSMM), a cloud resource management module (CRMM) and a cloud security management module (CSEMM). Each of these modules should be considered in three dimensions (technology, management and effectiveness) as stated. Each module has its own maturity requirements, and is linked to the other modules to allow construction of the overall maturity requirement framework of cloud computing.

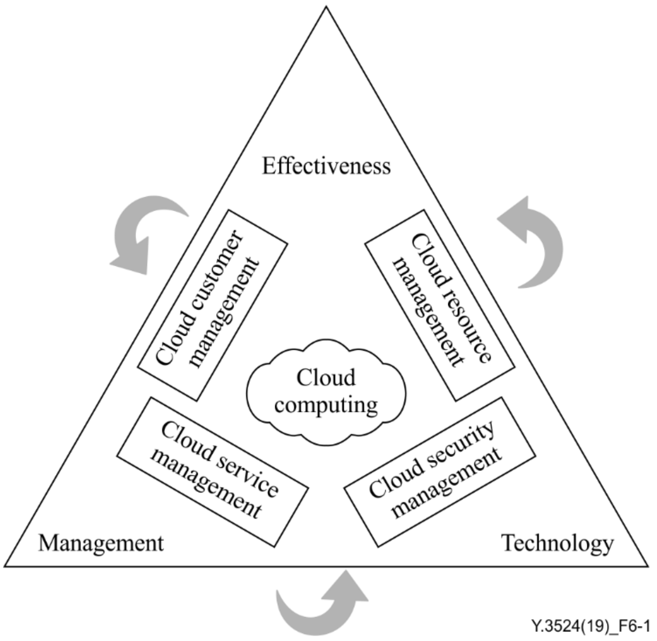


Figure 6-1 – The cloud computing maturity model

In order to evaluate the cloud computing maturity, there are several matrices in the cloud computing maturity model. Table 6-1 presents indicators used in the cloud computing maturity model. The indicators and their descriptions are as follows: "T" refers to technology indicator, "M" refers to management indicator, "E" refers to effectiveness indicator.

Table 6-1 – Indicators in cloud computing maturity model

Module	Indicator	Description	T	M	E
Cloud customer management	Resource cost utilization of cloud	It is the key measurement of capital investment and cloud resource utilization. It represents the cloud resource usage per unit cost.			√
	Cloud service design and deployment	It is the total time needed for design and deployment cloud service by CSP according to CSC's requirements.		√	
Cloud resource management	Resource sharing scale	It is the number of shared resources in resource pool providing multiple services to CSC, according to the statistics of tangible equipment entities such as physical machine, storage equipment, network equipment and other tangible entities.	√		
	Openness ability	It is the number of application programming interfaces (APIs) exposing the cloud service capabilities, including resource request, services configuration, etc.	√		

Table 6-1 – Indicators in cloud computing maturity model

Module	Indicator	Description	T	M	E
	Physical machine cluster CPU average utilization	It is the average CPU utilization of physical machines in the resource pool, which reflects the overall CPU resource usage of the cloud. It could be calculated in given period of time (e.g., monthly, daily) average and the data can be obtained from the CSP.			√
	Physical machine cluster CPU peak utilization	It is the peak CPU utilization of physical machines in the resource pool, which reflects the max resource usage of the cloud. It could be calculated in given period of time (e.g., monthly, daily) average and the data can be obtained from the CSP.			√
	Physical machine memory utilization	It is the memory utilization of physical machines in the resource pool, which reflects the overall memory resource usage of the cloud. It could be calculated in given period of time (e.g., monthly, daily) and the data can be obtained from the CSP.			√
	Average virtualization integration	It is the ratio of the total number of virtual machines to the total number of the virtualized servers in resource pool. This indicator reflects the level of virtualization application.		√	
	Resource pool virtualization	It is the ratio of host machines hosting the virtual machine to the total number of physical machines in a resource pool. This indicator reflects the virtualization degree.		√	
	Data storage pooling	It is the ratio of cloud storage resources capacity to the total storage resources capacity of the resource pool, including distributed block storage, object storage and distributed file storage, etc.		√	
	Computation resource specification	It is the specification providing the computation resource template (including QoS) according to computation unit and memory capacity, in which the resource capacity is variable and measurable.	√		
	Storage resource specification	It is the specification providing the storage resource template (including QoS) according to storage capacity, throughput or IOPS, in which the storage resource capacity is variable and measurable.	√		

Table 6-1 – Indicators in cloud computing maturity model

Module	Indicator	Description	T	M	E
	Management capability of computation administrator	It is the number of per capita computation capacity (physical of virtualized servers) of CSP with the support of management tools, which represents cloud computation resource management level.		√	
	Management capability of storage administrator	It is the number of per capita storage capacity of CSP with the support of management tools, which represents cloud storage resource management level.		√	
	Management capability of network administrator	It is the number of per capita network resource of CSP with the support of management tools, which represents cloud network resource management level.		√	
Cloud service Management	Cloud service delivery cycle	It is the time needed to deliver cloud service to CSC. It includes the time of resource allocation, cloud service delivery, cloud service deployment and cloud service adjustment.		√	
	Cloud service availability	It is the property of accessibility and usability for a cloud service. It represents the percentages of application interruptions due to the unavailability of cloud services.	√		
Cloud security management	Security incidents	It is the number of major security incidents referring to the incidents causing significant cloud service impact.			√

6.2 Definition of cloud computing maturity levels

According to the model presented in clause 6.1, the cloud computing maturity should be defined according to the appropriate development stage by using cloud computing. Table 6-2 presents cloud computing maturity levels.

Table 6-2 – Cloud computing maturity levels

	Management	**Technology**	**Effectiveness**
Level 1 – Discrete island	Vertical shaft IT management mode	Local, script, repeat	Resource scattered, long the cloud service cycle
Level 2 – Layered decoupling	Based on best practice service processes	Acquisition and monitoring, process engine, resource pooling, standardization	Different levels of resource sharing, IT infrastructure and application tiring, resource delivery and the cloud service cycle shortens
Level 3 – Service oriented	Service Process is clear, IT service oriented	Shared architecture, rich cloud management capabilities, platform gradually automated	High degree of resource sharing, the cloud service cycle is monthly
Level 4 – Competence systematization	Service oriented operation process system	Service-driven technology, decoupled architecture, stable development, enhanced automation capabilities	Various shared resource, the cloud service cycle is daily
Level 5 – Service integration	Automated processes worked closely with the application	Diversified pooled resources, automated adaptive architecture	Resource deployment on demand, the cloud service cycle becomes second level

Each level could be described in terms of technology, management and effectiveness as follows:

- **Level 1 – Discrete island**: This maturity level comprises the vertical shaft IT management mode. The system is local or partially based on cloud, each application has independent and scattered IT resources, such as repeat script, software and investment. It usually takes a long time to satisfy the CSC needs.
- **Level 2 – Layered decoupling**: This maturity level comprises the best practice service processes. The resource pool is standardized, equipped with the acquisition monitoring and process engine. Resource is shared at different levels, IT infrastructure and application are tiring, and the cloud service delivery cycle becomes shorter to satisfy the CSC needs.
- **Level 3 – Service oriented**: This maturity level comprises clear service processing which is service oriented. Technology is in shared architecture, there are several cloud management functions, the monitoring becomes a platform service in this service level, and the platform is gradually automated. A high degree of resources are shared, and the cloud service delivery cycles become a monthly level to satisfy the CSC needs.
- **Level 4 – Competence systematization**: This maturity level constructs a service oriented operation process system. Technology used at this level is service driven and the architectural structure is in stable development. The automation capability is enhanced. There are various shared resources, and the cloud service time becomes a daily level to satisfy the CSC needs.
- **Level 5 – Service integration**: This maturity level integrates automated management processes. There is an adaptive architecture with diversified resource pool. The resource is deployed on demand, and the cloud service cycle becomes a seconds level to satisfy the CSC needs.

7 Cloud computing maturity functional framework

The CCMM, CRMM, CSMM and CSEMM modules should be analysed in three dimensions comprising: technology, management and effectiveness. There are corresponding maturity requirements in each module, which facilitate each other to obtain the construction of the cloud computing maturity framework as shown in Figure 7-1.

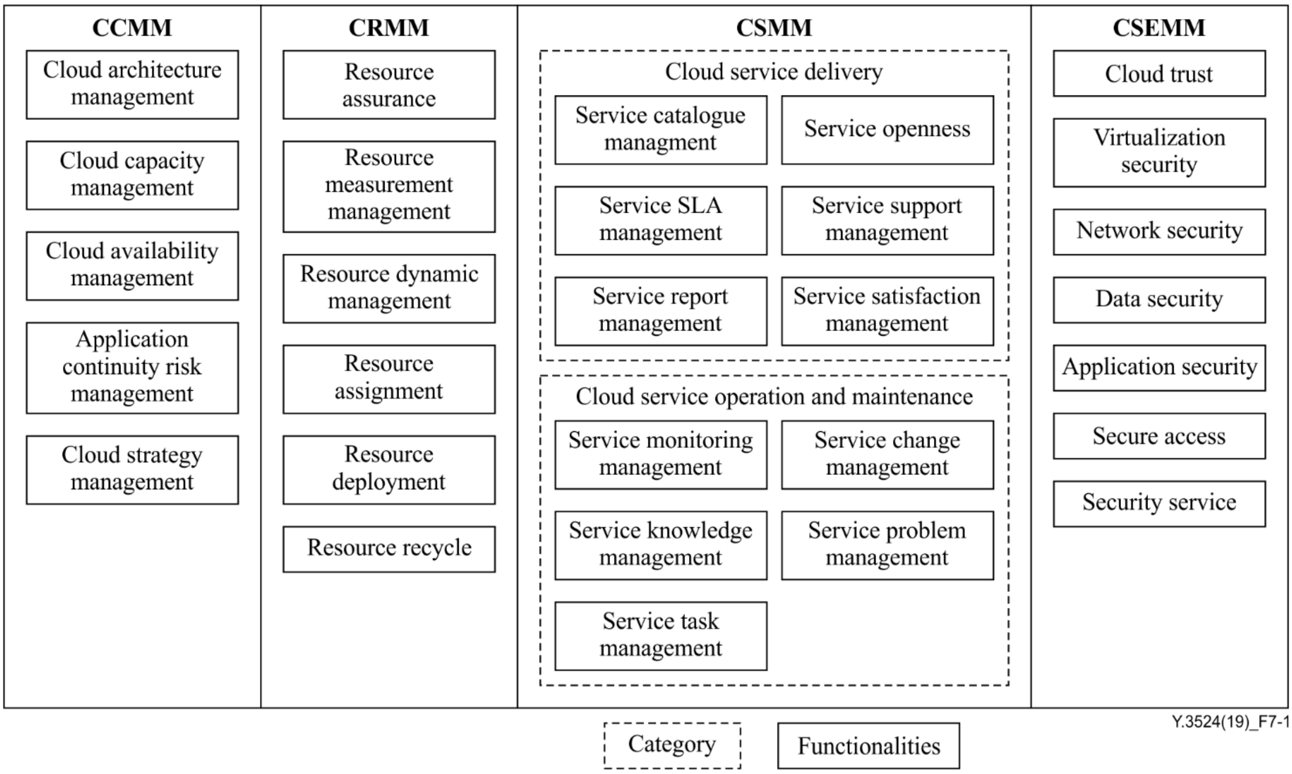

CCMM
Cloud architecture management
Cloud capacity management
Cloud availability management
Application continuity risk management
Cloud strategy management
CRMM
Resource assurance
Resource measurement management
Resource dynamic management
Resource assignment
Resource deployment
Resource recycle
CSMM
Cloud service delivery
Service catalogue managment
Service openness
Service SLA management
Service support management
Service report management
Service satisfaction management
Cloud service operation and maintenance
Service monitoring management
Service change management
Service knowledge management
Service problem management
Service task management
CSEMM
Cloud trust
Virtualization security
Network security
Data security
Application security
Secure access
Security service
Y.3524(19)_F7-1
Category
Functionalities

Figure 7-1 – Cloud computing maturity functional framework

7.1 Cloud customer management module (CCMM)

The CCMM undertakes the capability of cloud strategic planning, technical architecture planning, and service capability improvement for cloud services in the requirements analysis and procurement phase. All the functionalities aim to improve planning management effectiveness through the technologies and management method. It contains functionalities including the following:

1) **Cloud architecture management** – This functionality chooses the cloud architecture strategy, provides the evolution of cloud service, explores new technologies and updates the technical framework.

2) **Cloud capacity management** – This functionality performs the capacity planning for the entire resource pool and for applications and predicts the trend of capacity.

3) **Service availability management** – This functionality includes the virtual dynamic migration to ensure cloud service continuity and performs the cloud management data, application data and network backup and recovery.

4) **Application continuity risk management** – This functionality carries out risk analysis, identifies important service interruption risks, makes plans for the cloud service continuity risk and conducts regular exercises.

5) **Cloud strategy management** – This functionality performs cloud strategy selection and architecture and cost comparison services in order to improve the resource cost utilization of the cloud.

NOTE – Cloud strategy includes multiple cloud strategies such as single cloud or hyper cloud, etc.

7.2 Cloud resource management module (CRMM)

The role of the CRMM is to dispose and manage cloud resource information including capabilities, types and usage. This module ensures the cloud resource ability and quality provided by the resource pool. All the functionalities aim to improve cloud resource management effectiveness through the technologies and management method. It contains functionalities including the following:

1) **Resource assurance** – This functionality covers the assurance management of resources in support of cloud services including resource performance management, resource fault management and resource test management. For more information see clause 10.4.2 of [ITU-T Y.3521].

2) **Resource measurement management** – This functionality collects the measurement data including configuration data and performance data during the resource management lifecycle and performs data-driven ability.

3) **Resource dynamic management** – This functionality performs dynamic migration, expansion or shrinkage of applications in different clusters according to the system load calculation to ensure the level of cloud service.

4) **Resource assignment** – This functionality chooses suitable resources to allocate the cloud service.

5) **Resource deployment** – This functionality orchestrates a set of cloud resources and makes them available online to the CSC:cloud service user.

6) **Resource recycle** – This functionality carries out resource recycling, data release and charging termination.

7.3 Cloud service management module (CSMM)

The CSMM consists of user-oriented cloud service delivery works and system-oriented operation and maintenance works, which reflect the overall maturity level of a cloud service. All the functionalities aim to improve cloud service management effectiveness through the technologies and management method. The CSMM should be considered from the perspective of the cloud service delivery category and cloud service operation and maintenance category.

For the category of **cloud service delivery**, the CSMM contains functionalities including the following:

1) **Service catalogue management** – This functionality includes service catalogue management and service inventory management. For more information see clause 10.3.3.1 of [ITU-T Y.3521].

2) **Service openness** – This functionality offers APIs or function libraries for accurate cloud interoperability and portability.

3) **Service SLA management** – This functionality offers capabilities for managing the service levels of a particular cloud service For more information see clause 9.2.5.3.6 of [ITU-Y.3502].

4) **Service support management** – This functionality focuses on customer relationship management, and performs service desk and incident solutions. It is responsible for receiving and processing service requests, assisting CSC, and coordinating with specialist support groups.

5) **Service report management** – This functionality generates services usage reports according to the type of cloud service catalogue and specification based on monitor data

and the measurement of information. It could offer cloud usage service optimization advice to CSC.

6) **Service satisfaction management** – This functionality performs the service satisfaction survey and analysis of CSC:cloud service user action data and offers cloud service optimization recommendations to CSP.

For the category of **cloud service operation and maintenance**, the CSMM contains functionalities including the following:

1) **Service monitoring management** – This functionality provides monitoring and reporting on functional components. For more information see clause 9.2.5.3.3 of [ITU-Y.3502].

2) **Service change management** – This functionality responds to manage the service change, ensures that the corresponding changes are recorded and assessed, and approves changes for the corresponding sorting, planning, testing, implementation and evaluation.

3) **Service problem management** – This functionality identifies and records problems, creates the problem list, classifies and tracks the problem from the degree of importance, urgency and priority. For more information see clause 10.3.2.1 of [ITU-Y.3521].

4) **Service knowledge management** – This functionality records, shares and transfers all the relevant knowledge about operation and maintenance in the summary of technical maintenance logs, operation manuals, etc.

5) **Service task management** – This functionality performs regular inspection, routine operations, patch management, batch processing and other routine tasks on a regular basis and manages the implementation of the inspection report.

7.4 Cloud security management module (CSEMM)

The CSEMM is a guarantee of reliable operation in single cloud, of cloud trust management in multiple cloud and covers the cloud management lifecycle. All the functionalities aim to improve cloud security management effectiveness through the technologies and management method. It contains functionalities including the following:

1) **Cloud trust management and mechanism** – This functionality defines the security areas and performs the mechanism of the workloads and data migration in inter-cloud, and performs trust cloud management to ensure security in multiple cloud.

2) **Virtualization security** – This functionality provides a virtual machine image file encryption storage and integrity check function to prevent malicious tampering with the image file. It performs the virtualized resource isolation between physical machines and offers virus protection ability.

3) **Network security** – This functionality identifies attacks between virtual machines, or external networks in the data centre network by traffic detection.

4) **Data security** – This functionality identifies the sensitive data types and defines them to perform privacy protection. It authorizes and performs data access control to preserve data integrity.

5) **Application security** – This functionality integrates security tools into the cloud developer's environment and finds and fixes security vulnerabilities in application running time.

6) **Secure access** – This functionality provides critical user and resource access management for cloud service by identity and access management (IAM) and authentication support.

7) **Security service** – This functionality offers various security cloud services to CSC such as firewall, anti-distributed denial of service (anti-DDoS), IAM service, security inventory, etc.

8 Cloud computing maturity requirements

This clause provides cloud computing maturity requirements derived from the use cases described in Appendix I.

8.1 Cloud customer management maturity requirements

This clause provides cloud computing maturity requirements related to cloud customer management maturity.

8.1.1 Cloud architecture management

It is recommended that CSP provides openness and modular architecture to support heterogeneous resource and inter-cloud trust management.

8.1.2 Cloud capacity management

It is recommended that CSP provides capacity measurement data and performs capacity forecasting in higher maturity level.

8.1.3 Resource cost utilization of cloud

It is recommended that CSP supports resource usage optimization to improve the resource cost utilization of cloud.

8.1.4 Cloud availability management

It is recommended that CSP provides a data backup and recovery service in relation to the business continuity and disaster recovery (BC/DR) policy.

8.1.5 Application continuity management

It is recommended that CSP supports application continuity practice in multi-cloud or inter-cloud to ensure service stability and reliability.

8.1.6 Cloud strategy management

It is recommended that CSP adjusts cloud strategy planning to fit the CSC's demands.

NOTE – The cloud strategy planning includes but is not limited to multi-cloud, inter-cloud.

8.2 Cloud resource management maturity requirements

This clause provides cloud computing maturity requirements related to cloud resource management maturity.

8.2.1 Resource measurement management

It is recommended that CSP supports continuously updating of the configuration and measurement data.

NOTE – The configuration and measurement data includes available resources and performance data.

It is recommended that CSP supports openness and availability of cloud resources and its utilization data by APIs or other forms.

8.2.2 Resource dynamic management

It is recommended that CSP automates resource scheduling.

8.2.3 Resource assignment

It is recommended that CSP provides automation for cloud resource assignment.

8.2.4 Resource deployment

It is recommended that CSP provides automation for cloud resource deployment.

8.2.5 Resource recycle

It is recommended that CSP provides automation for cloud resource recycle.

8.3 Cloud service management maturity requirements

This clause provides cloud computing maturity requirements related to cloud service management maturity.

8.3.1 Service catalogue management

It is recommended that CSP supports cloud service catalogue management.

It is recommended that CSP supports customization of cloud service catalogues to distinguish diversity in cloud services.

8.3.2 Service openness

It is recommended that CSP provides cloud service APIs.

8.3.3 Service support management

It is recommended that CSP provides cloud service support.

NOTE – The cloud service support includes but is not limited to a support desk or automation chatbot.

It is recommended that CSP supports unified maintenance framework in encapsulated manner.

NOTE – The unified maintenance framework includes but is not limited to agent, operations libraries, runtime libs and deployment toolsets, etc.

8.3.4 Service report management

It is recommended that CSP provides a monitoring and charging report including actual resource utilization distribution, average utilization and peak utilization.

8.3.5 Service satisfaction management

It is recommended that CSP supports a satisfaction survey to enrich and improve their cloud service.

8.3.6 Service change management

It is recommended that CSP establishes continuous integration and continuous deployment to support change management process.

8.3.7 Service problem management

It is recommended that CSP supports recording the service problems, maintaining the service problems list and classifying the service problems according to urgency and priority.

8.3.8 Service knowledge management

It is recommended that CSP establishes a knowledge management database to offer frequently asked questions (FAQ).

It is recommended that CSP establishes a strategy knowledge database to enhance the maintenance ability.

NOTE – The strategy knowledge includes but is not limited to abnormal detection, stop-loss strategy, root cause analysis and capacity forecast, etc.

8.3.9 Service task management

It is recommended that CSP assigns the questions or problems of CSC into tasks and records, organizes into tracks and executes them in a task management process.

8.4 Cloud security management maturity requirements

This clause provides cloud computing maturity requirements related to cloud security management maturity.

8.4.1 Cloud trust management

It is recommended that CSP supports inter-cloud trust management to leverage migration towards multi-cloud.

8.4.2 Virtualization security

It is recommended that CSP supports east-west traffic control between virtual machines.

It is recommended that CSP supports fault isolation between virtual machines.

8.4.3 Network security

It is recommended that CSP supports the network traffic isolation among the CSCs application.

8.4.4 Data security

It is recommended that CSP imposes data control in rest and in transit.

It is recommended that CSP supports data encryption, data integrity authentication, software and data signing and secure time-stamping.

8.4.5 Secure access

It is recommended that CSP supports an IAM service which provides secure access to the user layer of the virtualization stack, platform and application service.

8.4.6 Security service

It can be optional that the CSP provides the configuration security baseline for OS and platform services.

It is recommended that CSP supports various security services.

NOTE – The security service includes but is not limited to block chain service, code audit and security evaluation.

9 Security considerations

Security aspects for consideration within the cloud computing environment, including cloud security management phase in could computing maturity consideration, are described in

[ITU-T X.1601], which analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

Appendix I

Use case of cloud computing maturity

(This appendix does not form an integral part of this Recommendation.)

I.1 Use case template

The use cases developed in Appendix I should adopt the unified format presented in Table I.1 for better readability and convenient material organization.

Table I.1 – Use case unified format template

Title	The title of the use case
Description	Scenario description of the use case
Roles	Roles involved in the use case
Figure (optional)	Figure to explain the use case, but not mandatory
Pre-conditions (optional)	The necessary pre-conditions that should be achieved before starting the use case.
Post-conditions (optional)	The post-condition that will be carried out after the termination of current use case.
Derived requirements	Requirements derived from the use cases, whose detailed description is presented in the dedicated chapter

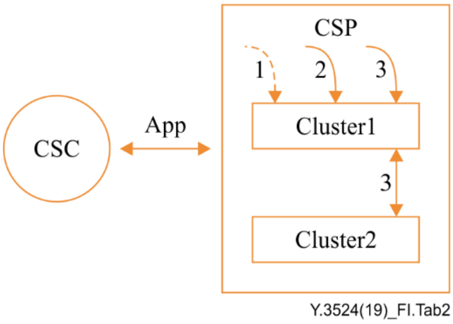
I.2 Use case on resource dynamic management

This use case presented in Table I.2 illustrates the resource dynamic management as a requirement. It is an example in a resource management phase.

Table I.2 – Resource dynamic management

Title	Resource dynamic management
Description	– The CSC requests to deploy a new application in cloud. – The CSP provides the cloud resource in 2 resource clusters. – The purpose of CSC is to make full use of cloud resources and run application quickly – CASE1: CSP: cloud service manager **manually** chooses the cluster which has lower resource utilization to deploy the application. – CASE2: CSP: cloud service manager **automatically** chooses the cluster which has lower resource utilization to deploy the application with the help of cloud platform. – CASE3: CSP: cloud service manager **automatically** chooses the cluster which has lower resource utilization to deploy the application with the help of cloud platform. In order to load balance, the application might provision between the 2 clusters **automatically**. Take the resources utilization and efficiency as an important issue, CASE3 is the best way to resource dynamic management, and CASE2 better, CASE1 is common.

Table I.2 – Resource dynamic management

Roles	CSC, CSP
Figure (optional)	 CSP 1 2 3 Cluster1 3 Cluster2 CSC App Y.3524(19)_FI.Tab2
Pre-conditions (optional)	– The CSP can gain the resource utilization data for the cluster. – The CSC's application is in dynamic load. – The CSP allocate resources according to current resource utilization.
Post-conditions (optional)	
Derived requirements	– Resource dynamic management (refer to clause 8.2.2)

I.3 Use case on cloud capacity management

This use case presented in Table I.3 illustrates the cloud capacity management as a requirement. It is an example in a cloud customer management phase.

Table I.3 – Cloud capacity management

Title	Cloud capacity management
Description	In the requirements analysis and procurement phase, the CSC should choose the suitable cloud type (such as private cloud, hyper cloud or public cloud etc.), the resource type (such as virtual machine specification, storage, cloud mode and etc.) and calculate the total resource quantity in order to purchase or construct the enough cloud service in the resource pool. CSC should make sure of the final cloud capacity to meet the needs of a certain period of time for business development. – CASE1: Each CSC: cloud service user estimates and forecasts its own needs. CSC:cloud service administrator collects the requirement and quantity form business applications over the cloud off-line following the process manually. – CASE2: CSC: cloud service administrator accurately collects performance and current cloud capacity measurement data (such as resource utilization) form CSP, who can help to identify current resource capabilities based on benchmarks, quantifies resource performance, and performs capacity forecasting through status analysis and capacity early warning information. – CASE3: CSC: cloud service administrator is not only forecasts the capacity basing on the cloud resource data of capabilities but also could combine with the data from CSC:cloud service user on-line or off-line pressure measurement, in order to make sure the balance of cloud service performance and actual business performance on demand.

Table I.3 – Cloud capacity management

	For the capacity planning and forecasting and budget control， CASE3 is the best way for cloud capacity management, and CASE2 is better, CASE1 is common.
Roles	CSC, CSP
Figure (optional)	/
Pre-conditions (optional)	– The CSC has already run some of applications in cloud. – The CSP provides the regular cloud resource for CSC. – The CSP could provide necessary monitoring data for CSC. – The CSC could make pressure measurement on-line or off-line for the application over the cloud.
Post-conditions (optional)	The cloud capacity which CSC purchases or constructs in cloud customer phase could meet the need of a certain period of time for business development.
Derived requirements	– Cloud capacity management (refer to clause 8.1.2)

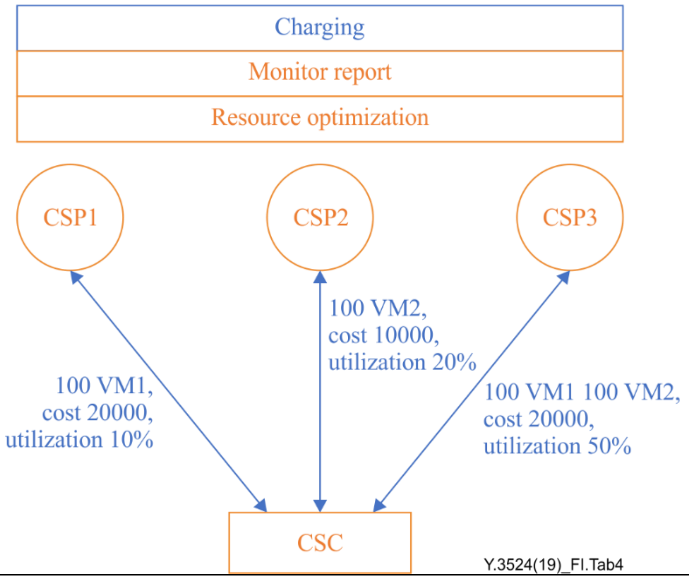
I.4 Use case on resource cost utilization of cloud

This use case presented in Table I.4 illustrates the resource cost utilization as a requirement in the cloud customer management phase.

Table I.4 – Resource cost utilization of cloud

Title	Resource cost utilization of cloud
Description	CSC should control the expenditures in budget and meet as many business demands as possible and CSP will to attract more CSC for more incomings by improving the resource utilization. So resource cost utilization of cloud, which is the metric for measuring the effectiveness of investment by considering both expenditures and resource utilization, is the issue to be considered. The CSC determines the cloud resource capacity to purchase including the numbers of suitable cloud services and service availability requirements for SLA. The CSP offers the cloud service catalogue and provides purchase suggestions and resource usage optimization recommendations. After a period of cloud service operation time, the CSP will provide the charging and monitoring report including actual resource utilization distribution, average utilization, peak utilization, and also some resource usage optimization recommendations such as service specifications matching. CSC could optimize next procurement plan. As example, there might be different cases as follows： – CASE1: CSP1 provides 100 virtual hosts in higher performance and cost 20000. In that case CSP could supports CSC's application load 100. The actual host average utilization is only 10% in given period of time. – CASE2: CSP2 provides 100 virtual hosts in common performance in the lowest costing 10 000 using less hosts than CSP1. In that case CSP could support CSC's same application load 100. The actual host average utilization is 20% in a given period of time. In this case CSP2's resource

Table I.4 – Resource cost utilization of cloud

	cost utilization of cloud is better than CSP1, because it optimizes the resource usage by data analysis of historical resource utilization and reduces the provided resources. – CASE3: CSP3 provides 100 virtual hosts in higher performance and 100 virtual hosts in common performance with the same total cost 10 000 compared with CSP2. According the operation report and utilization distribution, the CSC plans to support more business requirements by mixing deployment of application1 (online application) and application2 (analysis application) to support more business. Therefore, the actual host average utilization is 50% over given period of time. In this case CSC3 resource service cost utilization is better than CSC2, because CSC3 could support more business requirements by mixing deployment applications at the same cost. To improve the resource cost utilization of cloud the higher it is, the more mature it is. Therefore, the CASE3 is the best method for resource cost utilization of cloud, and CASE2 is better, CASE1 is common.
Roles	CSC, CSP
Figure (optional)	 Charging Monitor report Resource optimization CSP1 CSP2 CSP3 100 VM2, cost 10000, utilization 20% 100 VM1, cost 20000, utilization 10% 100 VM1 100 VM2, cost 20000, utilization 50% CSC Y.3524(19)_FI.Tab4
Pre-conditions (optional)	– The CSC pays for the cloud service as actual usage and SLA.
Post-conditions (optional)	
Derived requirements	– Service report management (refer to clause 8.3.4) – Resource cost utilization of cloud (refer to clause 8.1.3)

I.5 Use case on cloud resource management

This use case presented in Table I.5 illustrates some requirements in cloud resource management.

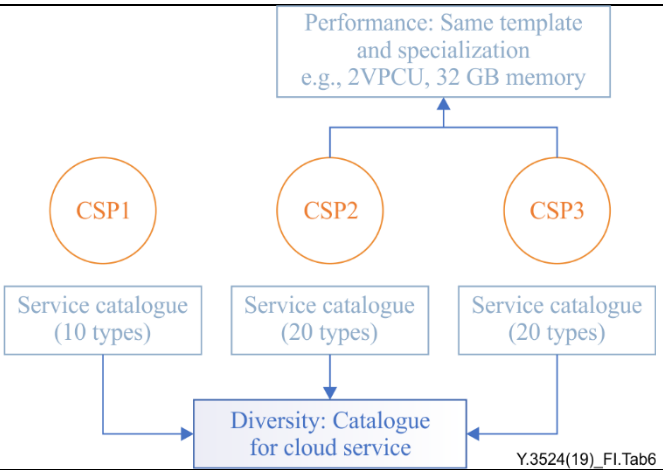
Table I.5 – Cloud resource management

Title	Cloud resource management
Description	The CSC needs specified cloud resources (IaaS service) to deploy its application on demanded types with specified quantity. – CASE1: CSP: cloud service manager could allocate and deploy the cloud resource to CSC off-line or manually. The total resource delivery cycle is **long**. And the CSP **rarely performs resource recycle** or resource release reminders proactively. The configuration and measurement data update on time after any resource change. – CASE2: CSP: cloud service manager could allocate and deploy the cloud resource to CSC automatically. The total resource delivery cycle is **short**. And the CSP could **inform resource release** to CSC and **act resource recycle** with the permissions of CSC. The configuration and measurement data update occurs after any resource change. – CASE3: CSC: cloud service administrator could allocate and deploy the cloud resource itself automatically with no interaction of CSP: cloud service administrator. The total resource delivery cycle is **short,** and the CSP cloud **automatically act resource recycle without any effect to the application**. The configuration and measurement data update occurs immediately after any resource change and can be consumed by the CSP or CSC to support the resource elasticity. According to the efficiency a of resource management, CASE3 is the best way for cloud resource management and CASE2 is better, CASE1 is common.
Roles	CSP, CSC
Figure (optional)	/
Pre-conditions (optional)	– The CSP provides the regular cloud resource for CSC.
Post-conditions (optional)	CSC could apply and adjust resources flexibly.
Derived requirements	– Resource assignment (refer to clause 8.2.3) – Resource deployment (refer to clause 8.2.4) – Resource recycle (refer to clause 8.2.5) – Resource measurement management (refer to clause 8.2.1)

I.6 Use case on cloud service catalogue management

This use case present in Table I.6 illustrates the cloud service catalogue management and service satisfaction management as requirements of cloud maturity management.

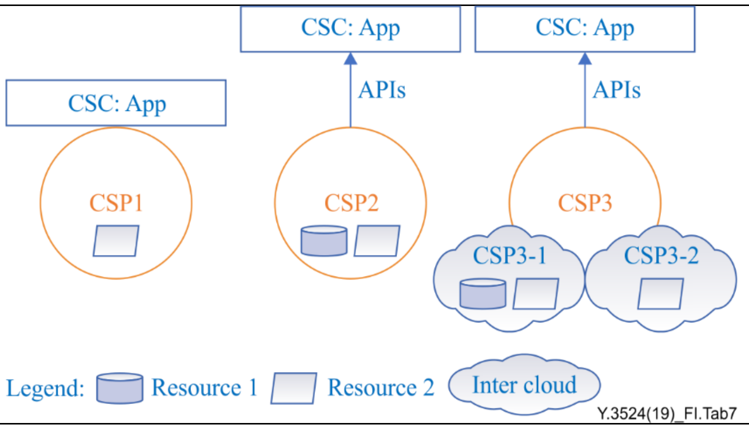
Table I.6 – Cloud service catalogue management

Title	Cloud service catalogue management
Description	The CSC chooses different cloud services form catalogues and the same cloud service template specification from different CSPs. – CASE1: CSP1's cloud service catalogue has published 10 cloud services, which don't have the service the CSC needs. – CASE2: CSP2's cloud service catalogue has published 20 cloud services, which is more various than CSP. The CSP frequently interview CSC needs and act CSC satisfaction survey to update cloud service catalogue and optimize the existed cloud service. – CASE3: CSP3 has the same number of cloud services to CSP2, but for the same cloud service template specification (e.g., a kind of VM with 2VCPUs and 32GB memory), the comprehensive performance of VM form CSP3 is better than the VM form CSP2 measured by the standard benchmark test. According to cloud resource capabilities form diversity and performance, comparison with the diversity of services CSP2 and CSP3 is better than CSP1.From performance perspective, CSP3 is better than CSP2 in the same template specification.
Roles	CSP, CSC
Figure (optional)	 Performance: Same template and specialization e.g., 2VPCU, 32 GB memory CSP1 CSP2 CSP3 Service catalogue (10 types) Service catalogue (20 types) Service catalogue (20 types) Diversity: Catalogue for cloud service Y.3524(19)_FI.Tab6
Pre-conditions (optional)	
Post-conditions (optional)	CSC would rather to choose the CSP which has various and high performance cloud services
Derived requirements	– Cloud service management (refer to clause 8.3.1) – Cloud service satisfaction management (refer to clause 8.3.5)

I.7 Use case on cloud architecture management and cloud service openness

This use case presented in Table I.7 illustrates the cloud architecture management and cloud service openness as requirements of cloud maturity management.

Table I.7 – Cloud architecture management and cloud service openness

Title	Cloud architecture management and cloud service openness
Description	The CSC needs to design and construct the cloud architecture themselves or with the support of CSP and makes cloud strategy of private or hybrid cloud. The architecture should consider the scalability, modularity and interoperability. CSC should consider the business continuity among multi-cloud. – CASE1: CSC's application relies on the specific cloud architecture. The existing cloud architecture used by CSP is closed and it could only integrate limited resources in cloud environment. There are no APIs exposed to CSC. – CASE2: CSP's cloud architecture is openness and could integrate multiple heterogeneous resources through APIs exposed to CSC. In this case, the CSC has better flexibility to use the cloud service by programming. – CASE3: CSP's cloud architecture is openness, support heterogeneous resource and inter-cloud trust management. CSC could implement the hybrid cloud management. There are APIs exposed to CSC and inter-cloud. In this case, the CSC has better flexibility to use the cloud service by programming as well as CSC could perform multiple cloud migration. CSC could act application continuity practice to ensure service stability and reliability. According to the cloud architecture design and cloud deployment models, the CASE3 is the best way for cloud architecture management as cloud service is openness, CASE2 is better, CASE1 is common.
Roles	CSP, CSC
Figure (optional)	 CSC: App CSC: App CSC: App APIs APIs CSP1 CSP2 CSP3 CSP3-1 CSP3-2 Legend: Resource 1 Resource 2 Inter cloud Y.3524(19)_FI.Tab7
Pre-conditions (optional)	– CSC prefers to deploy the applications in different places or different clouds CSP providers.
Post-conditions (optional)	
Derived requirements	– Cloud architecture management (refer to clause 8.1.1) – Application continuity management (refer to clause 8.1.5) – Cloud strategy management (refer to 8.1.6) – Cloud service openness (refer to clause 8.3.2)

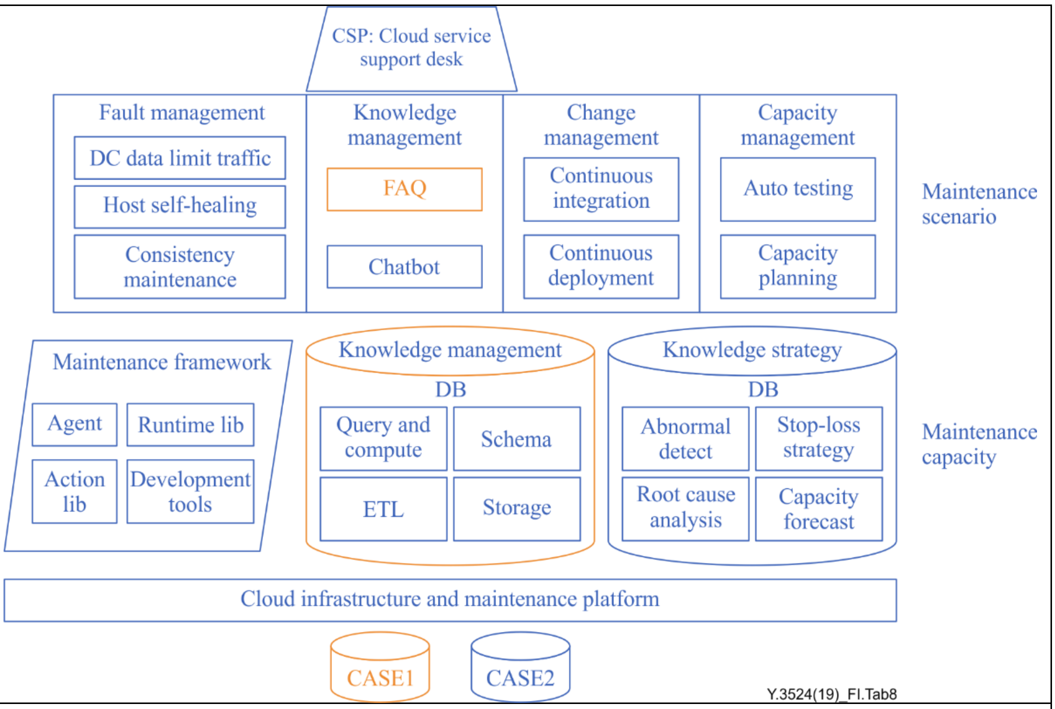
I.8 Use case on cloud service operation and maintenance management

This use case presented in Table I.8 illustrates requirements in cloud service operation and maintenance management.

Table I.8 – Cloud service operation and maintenance management

Title	Cloud service operation and maintenance management
Description	The CSP provides the cloud service support by support desk. There will be many maintenance capacities and various advanced scenarios to guarantee the cloud SLA in cloud infrastructure and maintenance platform. – CASE1: CSC requests a question or problem to CSP. The CSP records it to the problem list and assigns it into a task according urgency and priority, tracks and executes it. After the extract-transform-load (ETL) of the source data process, The CSP has established a knowledge management data base (DB) to support frequently asked questions (FAQ) to deal with the CSC's service request. The CSP: customer support and care representative cloud deal with the task. – CASE2: CSP builds a knowledge strategy database including abnormal detect, stop-loss strategy, cause analysis and capacity forecast by algorithm training data. The cloud service could be partially support by chatbot. Operation and maintenance capabilities can be encapsulated into a unified framework, including agent, operations libraries, runtime libraries and deployment toolsets. Base on the framework, knowledge management DB and knowledge strategy DB, the CSP cloud construct better maintenance scenario. In particular, the fault management, data limit traffic, host self-healing and consistency maintenance could be implemented. The change management, continuous integration and continuous deployment are used to support frequently cloud service publishing and changing. In case of capacity management, auto testing and capacity planning is necessary to enhance accuracy. The CASE2 has more maintenance capacity and various scenario than CASE1, therefore the cloud service operation and maintenance cloud be more flexible and effective in CASE2.
Roles	CSP,CSC

Table I.8 – Cloud service operation and maintenance management

Figure (optional)	 CSP: Cloud service support desk Fault management DC data limit traffic Host self-healing Consistency maintenance Knowledge management FAQ Chatbot Change management Continuous integration Continuous deployment Capacity management Auto testing Capacity planning Maintenance scenario Maintenance framework Agent Runtime lib Action lib Development tools Knowledge management DB Query and compute Schema ETL Storage Knowledge strategy DB Abnormal detect Stop-loss strategy Root cause analysis Capacity forecast Maintenance capacity Cloud infrastructure and maintenance platform CASE1 CASE2 Y.3524(19)_FI.Tab8
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Service support management (refer to clause 8.3.3) – Service change management (refer to clause 8.3.6) – Service problem management (refer to clause 8.3.7) – Service knowledge management (refer to clause 8.3.8) – Service task management (refer to clause 8.3.9)

I.9 Use case on cloud security management and availability management

This use case presented in Table I.9 illustrates some requirements in cloud security management and availability management.

Table I.9 – Cloud security management and availability management

Title	Cloud security management and availability management
Description	There is a sharing security responsibility model to provide a trustworthy foundation for enterprise systems and individual application by establishing high standards for information security within the cloud, which requires CSC and CSP to work together towards security objectives. – CASE1: **Infrastructure service**: CSP mainly offers the IaaS catalogue including compute, storage and network services. The CSC can architect and build a cloud infrastructure using technologies similar to and largely compatible with on-premises solutions. In this case CSP only needs to configure and operate Identity and Access Management (IAM) system that provides access to the user layer of the virtualization stack and ensure the virtual machine east-west traffic and fault isolation. CSC owns the operating system credentials but CSP helps CSC bootstrap the initial access to the operating system. CSC imposes data control in rest and in transit, and acts data encryption, data integrity authentication, software and data signing and secure time-stamping. – CASE2: **Platform services**: CSP manages the underlying infrastructure and foundation services, the operating system and the application platform. In this case CSP offers the configuration security baseline for OS and platform service. CSP needs to configure and operate IAM that provides access to platform and application. CSP provides data backup and recovery tools. CSC is responsible to configure and use tools in relation to the BC/DR policy. CSC is responsible for the data and firewall rules for access to the platform service. – CASE3: **Abstracted security services**: CSP operates the infrastructure layer, the operating system, platforms and the access endpoints to store and retrieve data. All kinds of cloud service is integrated with CSP IAM. CSP imposes data control in rest and in transit, and acts data encryption, data integrity authentication, software and data signing and secure time-stamping. CSP keeps the network traffic isolation among the CSCs. CSP cloud offer various security service such as block chain service, code audit, security evaluation. CSP cloud carry the security consultation in trust cloud management and give the suggestion of cloud migration in multiple cloud. According to the sharing security responsibility model.CASE3 is the best way for cloud security management and CASE2 better, CASE1 is common.
Roles	CSP, CSC

Table I.9 – Cloud security management and availability management

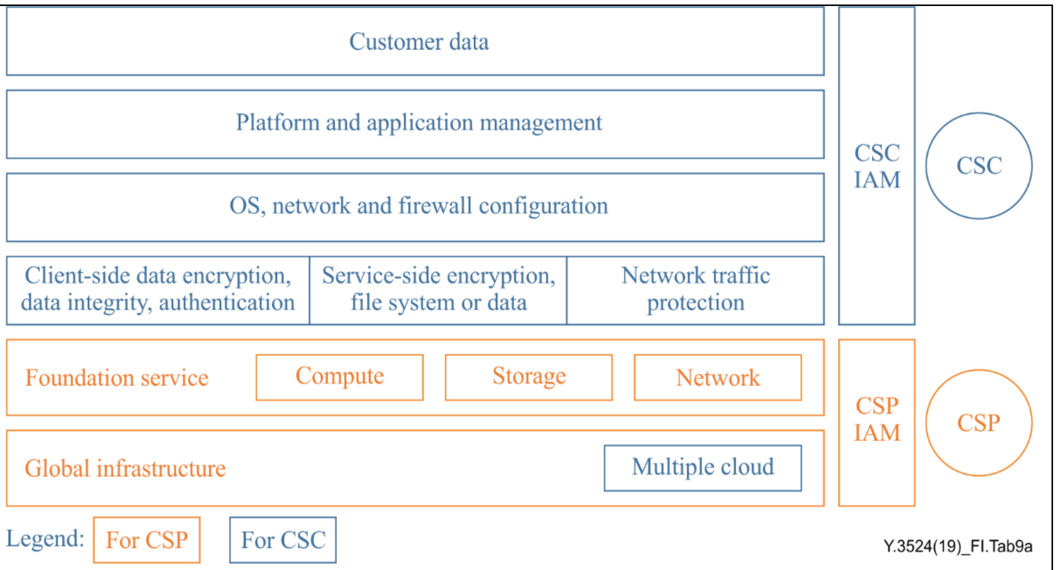
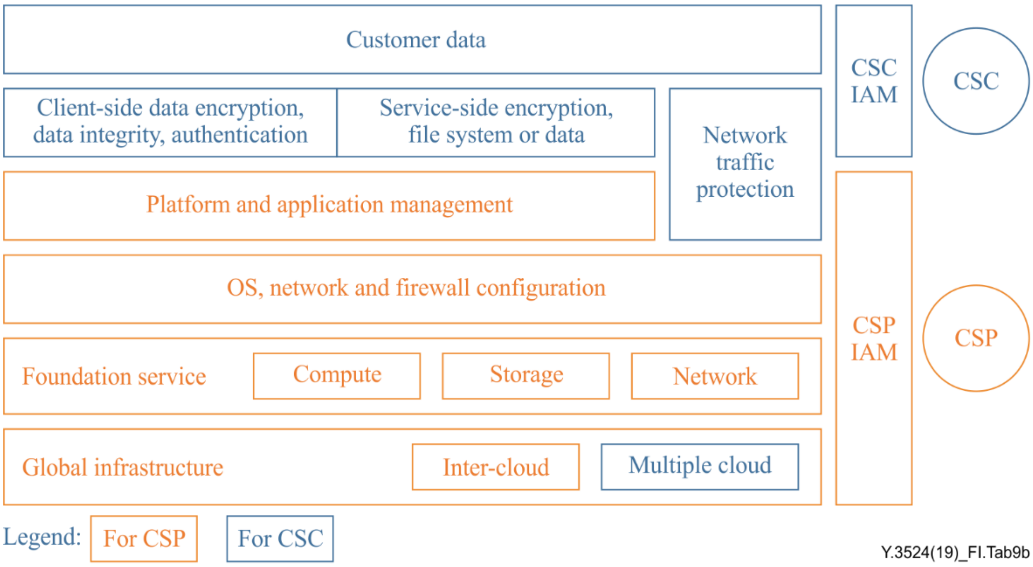
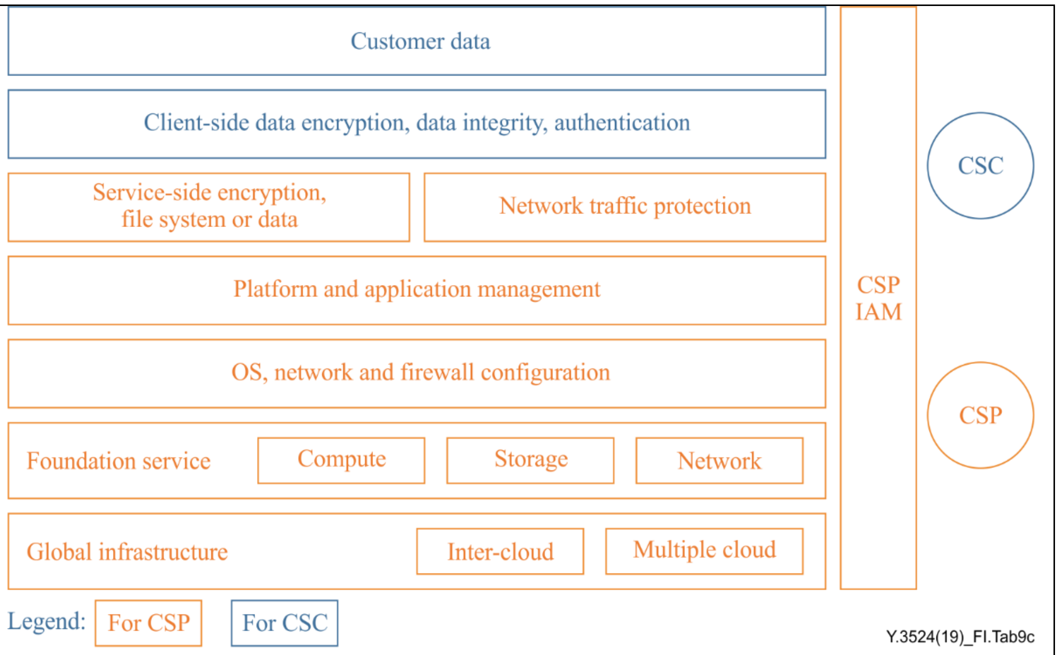
Figure (optional)	 Customer data Platform and application management OS, network and firewall configuration Client-side data encryption, data integrity, authentication Service-side encryption, file system or data Network traffic protection Foundation service Compute Storage Network Global infrastructure Multiple cloud CSC IAM CSC CSP IAM CSP Legend: For CSP For CSC Y.3524(19)_FI.Tab9a Case 1: Infrastructure service  Customer data Client-side data encryption, data integrity, authentication Service-side encryption, file system or data Network traffic protection Platform and application management OS, network and firewall configuration Foundation service Compute Storage Network Global infrastructure Inter-cloud Multiple cloud CSC IAM CSC CSP IAM CSP Legend: For CSP For CSC Y.3524(19)_FI.Tab9b Case 2: Platform service

Table I.9 – Cloud security management and availability management

	 Customer data Client-side data encryption, data integrity, authentication Service-side encryption, file system or data Network traffic protection Platform and application management OS, network and firewall configuration Foundation service Compute Storage Network Global infrastructure Inter-cloud Multiple cloud CSP IAM CSC CSP Legend: For CSP For CSC Y.3524(19)_FI.Tab9c Case 3: Security service
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Cloud trust management (refer to clause 8.4.1) – Virtualization security(refer to clause 8.4.2) – Network security(refer to clause 8.4.3) – Data security(refer to clause 8.4.4) – Security access (refer to clause 8.4.5) – Security service (refer to clause 8.4.6) – Cloud availability management (refer to clause 8.1.4)

Bibliography

[b-ITU-T Y.3520]	Recommendation ITU-T Y.3520 (2015), *Cloud computing framework for end to end resource management*.
[b-ISO/IEC/IEEE 42010]	ISO/IEC/IEEE 42010:2011, *Systems and software engineering – Architecture description*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020